P13602 W01

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 April 2002 (25.04.2002)

PCT

(10) International Publication Number
WO 02/33879 A2

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number: PCT/EP01/11888

(22) International Filing Date: 15 October 2001 (15.10.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0025435.9 17 October 2000 (17.10.2000) GB
60/242,451 24 October 2000 (24.10.2000) US

(71) Applicant *(for all designated States except US)*: TELEFONAKTIEBOLAGET L M ERICSSON (PUBL) [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: ANDERSON, Stefan [SE/SE]; Koltrastgränd 23, S-230 41 Klågerup (SE).

(74) Agent: O'CONNELL, David, Christopher; Haseltine Lake & Co., Imperial House, 15-19 Kingsway, London WC2B 1UD (GB).

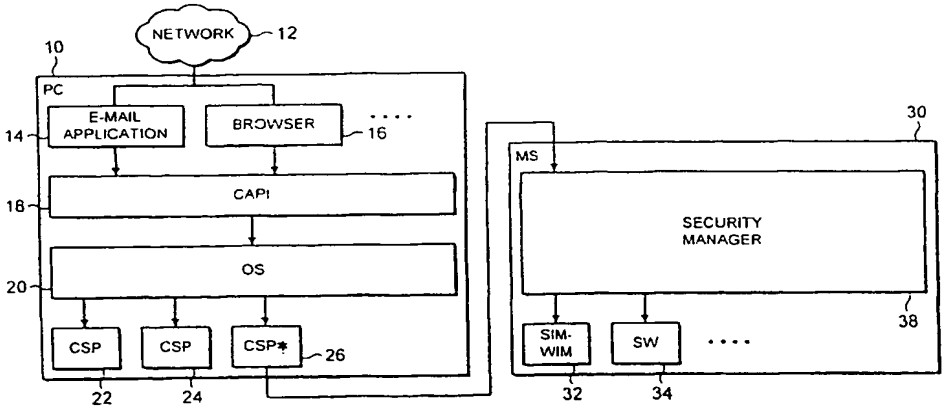
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECURITY SYSTEM



(57) Abstract: A communications device, which has a cryptographic module for use in mobile communications, can be used as a cryptographic services provider. For example, the device may be a device which can operate under the Wireless Application Protocol, that is, a WAP-enabled device, such as a mobile phone. This has the advantage that WAP-enabled devices include components which are used in public key/private key cryptographic systems as a part of their standard communication functions. These components therefore advantageously allow the device to be used as a cryptographic services provider. Advantageously, the device can use Wireless Transport Layer Security (WTLS) for mobile communications, and employs its cryptographic module when in use as a cryptographic services provider.

WO 02/33879 A2

SECURITY SYSTEM

TECHNICAL FIELD OF THE INVENTION

This invention relates to computer systems, and in particular to the improvement of security in such systems. More specifically, the invention relates to a method for improving the security of communications, for example over a computer network, although it is also applicable to increasing the security of a computer system.

BACKGROUND OF THE INVENTION

US-5,689,565 describes a cryptography system architecture for a computer, which provides cryptographic functionality to support an application which requires cryptography. The cryptography system has a cryptographic application program interface (CAPI) which interfaces with the application to receive requests for cryptographic functions. The system further includes at least one cryptographic service provider (CSP) that is independent from, but dynamically accessible by, the CAPI. The CSP provides the cryptographic functionality and manages the secret cryptographic keys.

This system architecture is used in many applications in which data may desirably be transferred across unsecured computer networks such as the internet. For example, this architecture can be used in applications such as email clients, web browsers, etc. A similar architecture can be used for access control within a computer system, and for hard disc encryption.

US-6,038,551 describes a development of the architecture disclosed in US-5,689,565, in which the computer includes a card reader, and an integrated circuit card (IC card) stores the cryptographic keys used by the CSP in the computer, and can perform

is taken to specify the presence of stated features, integers, steps or components but does not preclude the presence or addition of one or more other features, integers, steps, components or groups thereof.

BRIEF DESCRIPTION OF DRAWINGS

Figure 1 is a block schematic diagram of a first system implementing the present invention.

Figure 2 is a flow chart showing the operation of the system of Figure 1.

Figure 3 is a flow chart showing in more detail a part of the operation illustrated in Figure 2.

Figure 4 is a block schematic diagram of a second system implementing the present invention.

Figure 5 is a block schematic diagram of a third system implementing the present invention.

Figure 6 is a flow chart showing the operation of the system of Figure 5.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Figure 1 is a block schematic diagram of a computer system, including a personal computer (PC) 10, only the relevant components of which are shown. It will be apparent that, in this embodiment of the invention, and in the other illustrated embodiments, any computer system can be used in exactly the same way as the PC 10.

The computer has a connection to an external network 12, for example through a modem (not shown). Of particular concern here is the situation where the computer 10 is connected to an unsecured network, such as the internet.

The computer 10 has various software applications which require external communication, such as an email application 14, and a web browser 16, which use Secure Socket Layer (SSL) and/or Transport Layer Security (TLS) security. In many cases, the information which

Transport Layer Security (WTLS) can be used. This provides confidentiality for users, by encrypting messages which are transmitted over the wireless interface, and also provides authentication, by means of digital certificates.

In order to provide this WTLS functionality, the WAP-enabled device 30 includes a cryptographic module, which uses an embedded public key and private key on handshake for authentication, then generates symmetric session keys, which are used to encode messages before transmission and to decode received messages.

For example, the phone 30 may also include a Subscriber Identity Module - Wireless Identity Module (SIM-WIM) card 32, which is used to identify the subscriber, and can contain the cryptographic module. Alternatively, the cryptographic module can be realised in hardware or in software 34 in the phone 30, or may be provided on an external smart card. In order to access the cryptographic module, the MS 30 includes a security manager module 38. The operation of these devices will be explained further below.

In accordance with preferred embodiments of the present invention, the cryptographic module of the phone, and other features which are used to provide secure communication using the Wireless Application Protocol, also allow the phone 30 to be provide some or all of the functionality of a cryptography service provider.

In the case where the cryptographic module is embodied in hardware, the necessary information is provided on an integrated circuit in the device.

Where the Wireless Public Key Infrastructure (WPKI) is used to distribute the parameters for WTLS, it can also be used to distribute the parameters required for use as a cryptography service provider.

provider and the MS are possible.

Figure 2 is a flow chart showing a method by which the PC 10 can use the cryptographic functionality in the mobile phone 30.

The procedure starts with step 100, in which the application in the PC 10, such as the email application 14 or web browser 16 determines that cryptographic functionality is required, and sends a command to the CAPI 18. The cryptographic functionality which is required may for example be encryption, decryption, hash generation, message signing, verification, key generation, certificate management, or random number generation. Other types of cryptographic functionality which may be provided are described in the PKCS#11 standard mentioned above.

In step 102, the CAPI selects an appropriate CSP to provide the cryptography function. In this case, the CAPI selects the CSP* 26, which can access the cryptographic module in the MS 30.

In step 104, the CAPI 18 establishes communication with the selected CSP* 26, and the CSP* 26 establishes communications with the MS 30. As discussed above, the communications between the PC 10 and MS 30 can advantageously be over a Bluetooth short range radio link.

In step 106, the operating system (OS) 20 verifies the authenticity of the CSP*. It will be noted that this step may be unnecessary if the authenticity of the CSP* has already been established as part of an earlier process. As an alternative, this step can be carried out earlier in the process, and other changes in the order of the illustrated steps are also possible.

In step 108, a message is passed from the CAPI 18 via the CSP* 26 to the MS 30, with details of the cryptographic operation which is required.

communication with the hard disc 52. Since the information which is stored on the hard disc may be confidential, the application restricts access thereto, so that only authorised persons can gain access to it.

As is conventional, therefore, the hard disc application 50 can call a cryptographic application program interface (CAPI) 18, which is provided on top of the operating system (OS) 20.

As is also conventional, the cryptographic application program interface (CAPI) 18 can access one or more cryptography service providers (CSPs) 22, 24.

Different cryptography service providers (CSPs) may, for example, use different cryptographic algorithms, and may be used for different purposes.

In accordance with the present invention, as described in more detail with reference to Figures 1-3, some or all of the functionality of a cryptography service provider is available on a separate device, namely a mobile station (MS) 30, and the CSP* 26 can call the required functionality from the MS 30.

The mobile station may be exactly as described with reference to Figures 1 and 3 above.

Figure 5 shows a further alternative system in accordance with the invention.

Again, the computer system is described with reference to a personal computer (PC) 60, but it will be apparent that any computer system can be used in exactly the same way as the PC 60.

The computer has a connection to an external network 12, for example through a modem (not shown) to an unsecured network, such as the internet.

The computer 60 has various software applications which require external communication, such as an email application 14, and a web browser 16, which use Secure Socket Layer (SSL) and/or Transport Layer Security

the Bluetooth short-range radio transmission protocol, although an infrared connection is also possible. The protocol for the connection can for example be based on AT commands, and provides security for those communications. The command set is advantageously a version of the command set defined in a standard such as PKCS#11, described in the document "PKCS#11 v2.10: Cryptographic Token Interface Standard", published by RSA Security Inc. and incorporated herein by reference, where the commands are redefined as AT commands.

Figure 6 is a flow chart showing a method by which the PC 60 can use the cryptographic functionality in the mobile phone 30.

The procedure starts with step 160, in which the application in the PC 60, such as the email application 14 or web browser 16 determines that cryptographic functionality is required, and sends a command to the PKCS#11 interface 70. The cryptographic functionality which is required may for example be encryption, decryption, hash generation, message signing, verification, key generation, certificate management or random number generation.

In step 162, the PKCS#11 interface 70 selects an appropriate CT to provide the cryptography function. In this case, the PKCS#11 interface 70 selects the CT* 76, which can access the cryptographic module in the MS 30.

In step 164, the PKCS#11 interface 70 establishes communication between the application and the selected CT* 76, and the CT* 76 establishes communications with the MS 30. As discussed above, the communications between the PC 60 and MS 30 can advantageously be over a Bluetooth short range radio link.

In step 166, a message is passed from the PKCS#11 interface 70 to the MS 30, calling the cryptographic

CLAIMS

1. A method of encrypting communications from a computer having an application program interface, the method comprising using a mobile communications device, which includes a cryptographic module for use in mobile communication, as a cryptographic service provider.

2. A method as claimed in claim 1, wherein the mobile communications device is a WAP-enabled device.

3. A method as claimed in claim 1 or 2, wherein the cryptographic module is that used by the mobile communications device for Wireless Transport Layer Security communications.

4. A method as claimed in claim 1, 2 or 3, comprising providing a wired connection between the mobile communications device and the computer.

5. A method as claimed in claim 1, 2 or 3, comprising providing a wireless connection between the mobile communications device and the computer.

6. A method as claimed in any of claims 1 to 5, comprising:

when the application program interface requires cryptographic functionality, calling a cryptographic service provider function in the mobile communications device.

7. A mobile communications device, comprising a cryptographic module, the cryptographic module being usable:

(a) for encoding wireless communications from the device;

(b) in a cryptographic service provider with an application program interface of a remote computer.

8. A mobile communications device as claimed in claim 7, having a short-range wireless communications transceiver, for sending signals to and receiving signals from the remote computer.

to said command.

19. A module for a personal computer, wherein, in response to the module receiving a first command from a cryptographic application program interface, indicating that it requires cryptographic functionality, the module sends a second command to a mobile communication device, such that the mobile communications device acts as a cryptographic service provider for said personal computer.

20. A method of encrypting computer communications, the method comprising using a separate mobile communications device, which includes a cryptographic module for use in mobile communication, as a cryptographic service provider.

21. A method as claimed in claim 20, wherein the mobile communications device is a WAP-enabled device.

22. A method as claimed in claim 20 or 21, wherein the cryptographic module is that used by the mobile communications device for Wireless Transport Layer Security communications.

23. A method as claimed in claim 20, 21 or 22, comprising providing a wireless connection between the mobile communications device and the computer.

24. A computer system, comprising:

a computer; and

a mobile communications device, including a cryptographic module,

the computer having at least one application which requires cryptographic functionality,

a first part of the required cryptographic functionality being provided in the computer, and a second part of the required cryptographic functionality being provided in the mobile communications device,

the computer and the mobile communications device having means for establishing a secure communications

device.

32. A method as claimed in claim 28, comprising using a cryptographic module realised in hardware in the mobile communications device.

33. A method as claimed in claim 28, comprising using a cryptographic module realised in software in the mobile communications device.

34. A method as claimed in claim 28, comprising using a cryptographic module provided on an external smart card which can be read by the mobile communications device.

35. A method as claimed in claim 28, comprising using a cryptographic module a Wireless Identity Module (WIM) card in said mobile communications device.

36. A computer system for supporting an application, the computer system comprising:

a cryptographic application program interface; and

a cryptography service provider,

wherein, when the cryptographic application program interface determines that the application requires cryptographic functionality, sends a command to the cryptography service provider, and

wherein the cryptography service provider has a communications link to a cryptographic module of a mobile communications device, the cryptographic module of the mobile communications device being usable to encrypt communications between the mobile communications device and a telecommunications network over a wireless interface, and

wherein the cryptography service provider can obtain the cryptographic functionality, required by the application, from the cryptographic module of the mobile communications device.

37. A system as claimed in claim 36, wherein the cryptographic module is realised in hardware in the

mobile communications device further comprising a security manager module for receiving commands from a computer system over a second interface, wherein, in response to suitable commands received from the computer system over the second interface, the security manager module requests a cryptographic function from the cryptographic module, and returns the results of the cryptographic function to the computer system over the second interface.

45. A mobile communications device as claimed in claim 44, wherein the security manager module responds to a command set defined in a standard PKCS#11, where the commands are redefined as AT commands.

46. A mobile communications device as claimed in claim 44, wherein the second interface is a Bluetooth short-range radio interface.

47. A module for a computer system, the module comprising:

an application interface for connection to a computer application; and

an external interface for connection to a mobile communication device containing a cryptographic module;

wherein, when the module receives from the application interface a request for a cryptographic function which the module is unable to provide, the module sends a command over the external interface to the mobile communications device to request the cryptographic function therefrom.

48. A module for a computer system as claimed in claim 47, wherein the module has some cryptographic functionality, and comprises means for determining in response to a request from the application interface whether it is able to provide the requested function cryptographic function.

49. A module for a computer system as claimed in

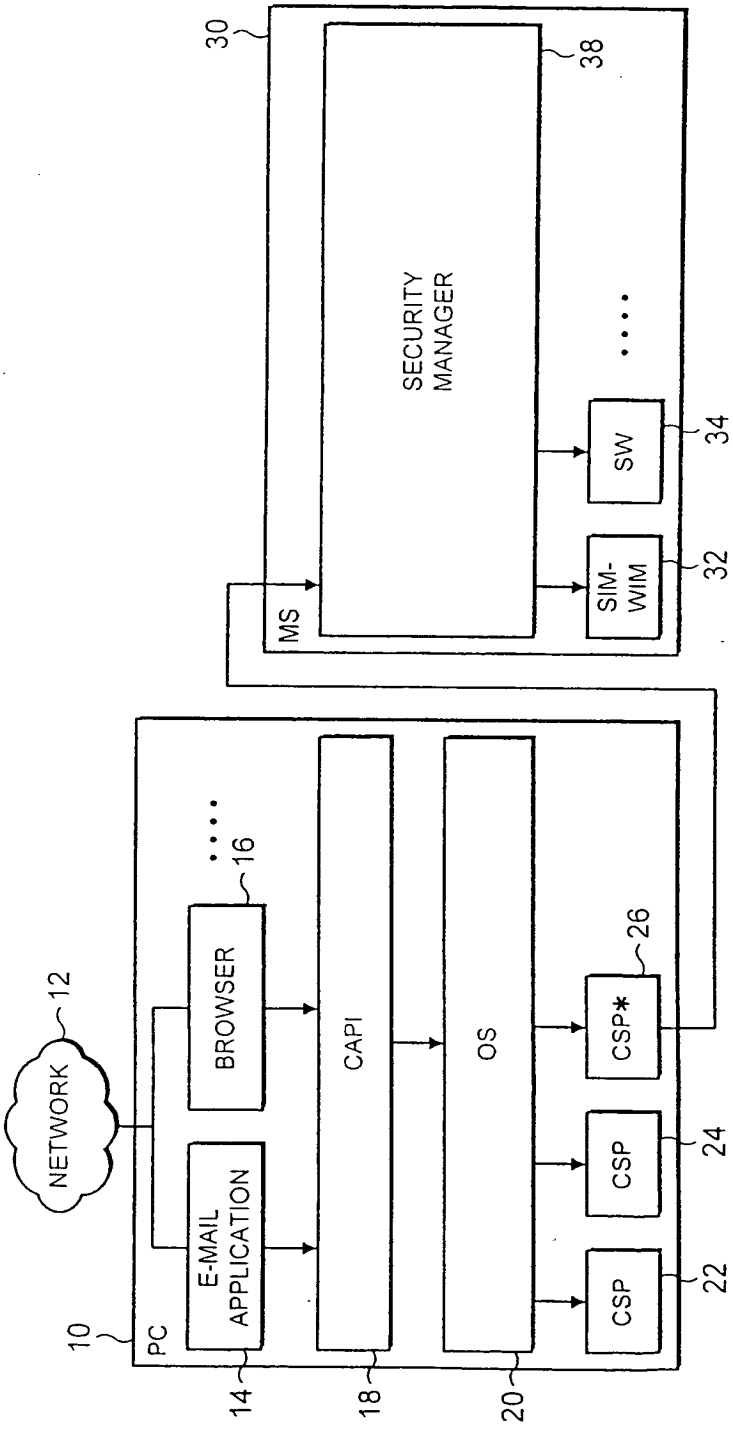

30
38
SECURITY MANAGER
MS
SW
34
SIM-WIM
32
12
NETWORK
BROWSER
16
E-MAIL APPLICATION
CAPI
OS
CSP*
26
CSP
24
CSP
22
10
PC
14
18
20

FIG. 1

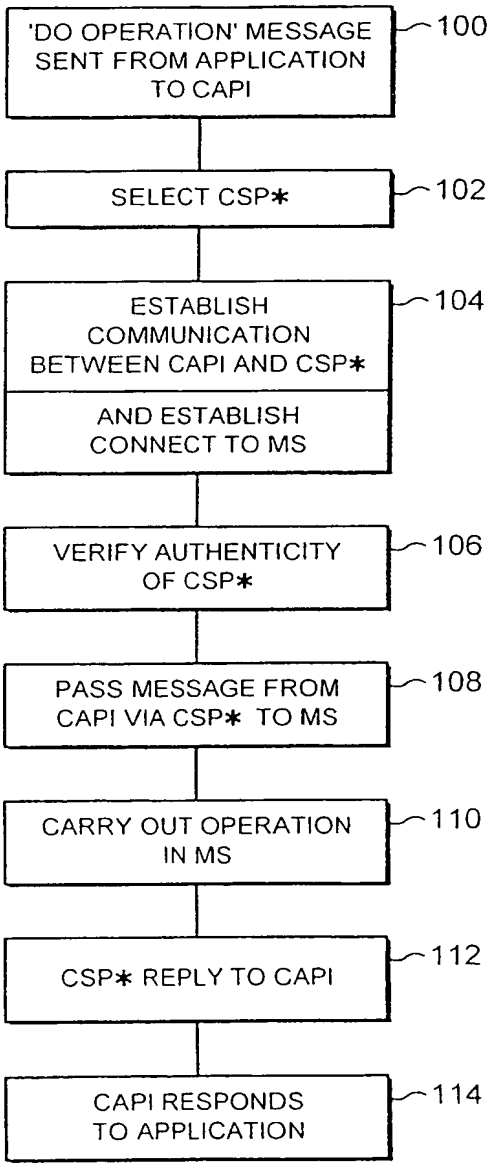

'DO OPERATION' MESSAGE SENT FROM APPLICATION TO CAPI
100
SELECT CSP*
102
ESTABLISH COMMUNICATION BETWEEN CAPI AND CSP*
AND ESTABLISH CONNECT TO MS
104
VERIFY AUTHENTICITY OF CSP*
106
PASS MESSAGE FROM CAPI VIA CSP* TO MS
108
CARRY OUT OPERATION IN MS
110
CSP* REPLY TO CAPI
112
CAPI RESPONDS TO APPLICATION
114

FIG. 2

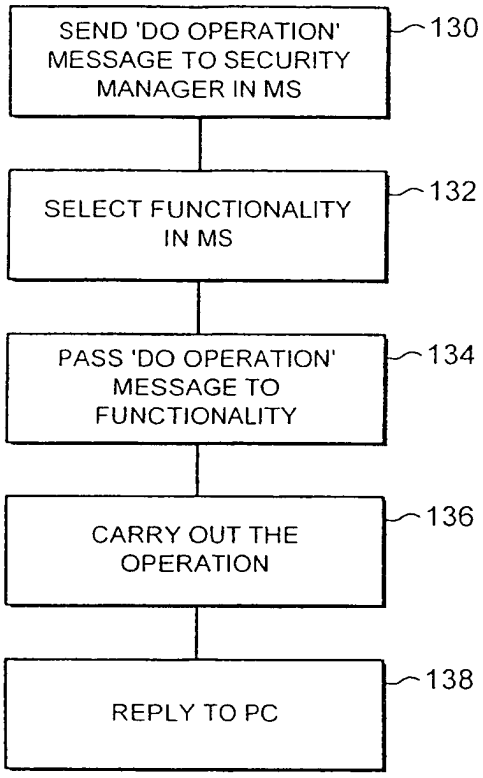

SEND 'DO OPERATION' MESSAGE TO SECURITY MANAGER IN MS
130
SELECT FUNCTIONALITY IN MS
132
PASS 'DO OPERATION' MESSAGE TO FUNCTIONALITY
134
CARRY OUT THE OPERATION
136
REPLY TO PC
138

FIG. 3

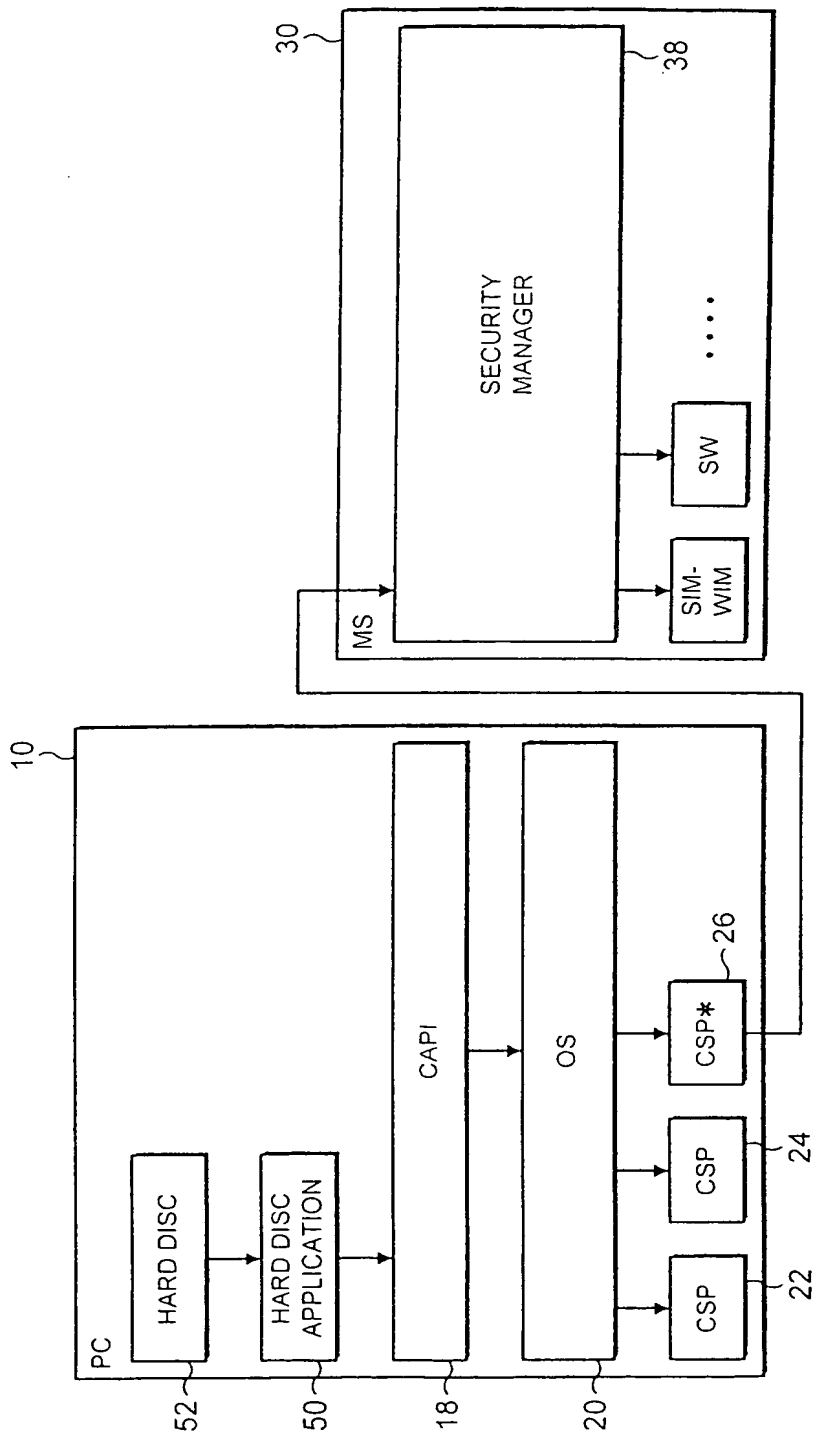

30
38
SECURITY MANAGER
SW
SIM-WIM
MS
10
PC
HARD DISC
HARD DISC APPLICATION
CAPI
OS
CSP*
26
CSP
24
CSP
22
52
50
18
20

FIG. 4

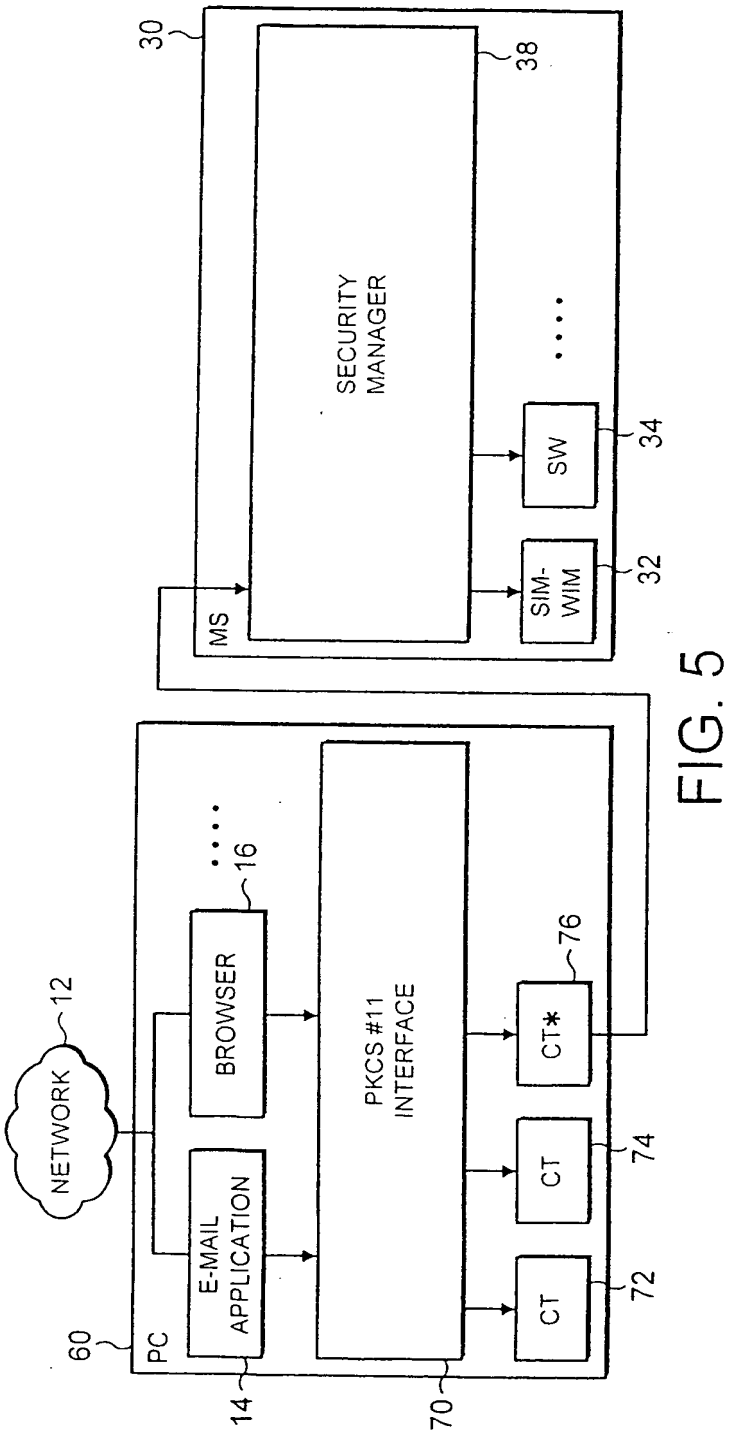

30
38
SECURITY MANAGER
SW
34
SIM-WIM
32
MS
12
NETWORK
BROWSER
16
E-MAIL APPLICATION
PKCS #11 INTERFACE
CT*
76
CT
74
CT
72
60
PC
14
70

FIG. 5

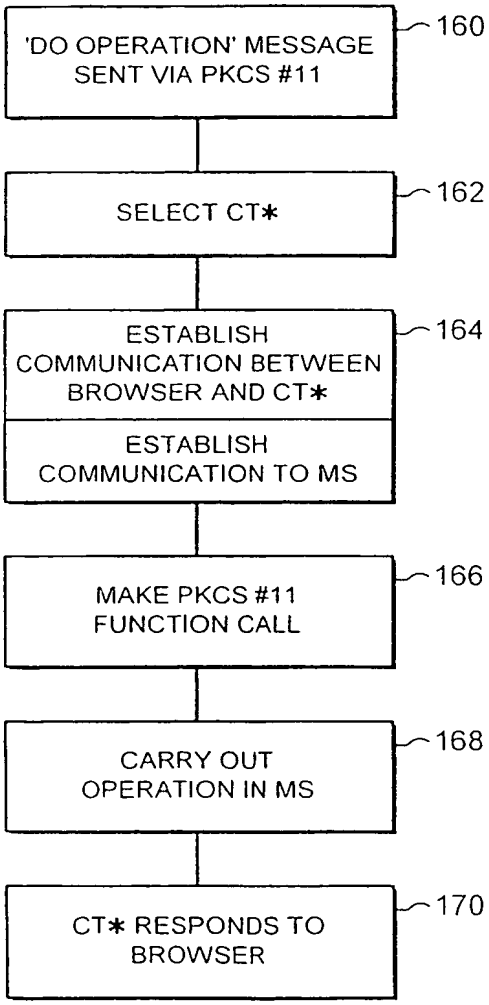

'DO OPERATION' MESSAGE SENT VIA PKCS #11
160
SELECT CT*
162
ESTABLISH COMMUNICATION BETWEEN BROWSER AND CT*
ESTABLISH COMMUNICATION TO MS
164
MAKE PKCS #11 FUNCTION CALL
166
CARRY OUT OPERATION IN MS
168
CT* RESPONDS TO BROWSER
170

FIG. 6

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	FOR FURTHER ACTION	see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.
HL76380/006		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/EP 01/11888	15/10/2001	17/10/2000

Applicant

TELEFONAKTIEBOLAGET L M ERICSSON (PUBL)

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 2 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

[ ] the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

[ ] contained in the international application in written form.

[ ] filed together with the international application in computer readable form.

[ ] furnished subsequently to this Authority in written form.

[ ] furnished subsequently to this Authority in computer readble form.

[ ] the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

[ ] the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. [ ] **Certain claims were found unsearchable** (See Box I).

3. [ ] **Unity of invention is lacking** (see Box II).

4. With regard to the **title**,

[X] the text is approved as submitted by the applicant.

[ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

[X] the text is approved as submitted by the applicant.

[ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. 1

[X] as suggested by the applicant.

[ ] because the applicant failed to suggest a figure.

[ ] because this figure better characterizes the invention.

[ ] None of the figures.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 01/11888

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 00 02406 A (NOKIA NETWORKS OY ;EKBERG JAN ERIK (FI)) 13 January 2000 (2000-01-13) page 2, line 21 -page 3, line 4	1-50
A	WO 00 20972 A (L 3 COMM CORP) 13 April 2000 (2000-04-13) abstract; claim 1	1-50
A	US 5 878 142 A (AMORUSO VICTOR P ET AL) 2 March 1999 (1999-03-02) column 2, line 21 - line 54	1-50

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 July 2002	05/08/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Veen, G

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 01/11888

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0002406 A	13-01-2000	FI 981565 A	08-01-2000
		AU 4912199 A	24-01-2000
		DE 19983405 T0	31-05-2001
		WO 0002406 A2	13-01-2000
		GB 2355157 A	11-04-2001
WO 0020972 A	13-04-2000	US 6151677 A	21-11-2000
		AU 6292999 A	26-04-2000
		EP 1149343 A2	31-10-2001
		WO 0020972 A2	13-04-2000
US 5878142 A	02-03-1999	US 5546463 A	13-08-1996
		US 5778071 A	07-07-1998